REMARKS

This application has been carefully reviewed in light of the Office Action dated October 26, 2006. Claims 1 to 15 remain in the application, of which Claims 1, 2, 11 and 13 to 15 are independent. Reconsideration and further examination are respectfully requested.

The abstract was objected to. A new abstract has been provided for as recited above. Withdrawal of the objection is respectfully requested.

Claim 9 was objected to as allegedly being a duplicate of Claim 1. The objection is traversed since Claim 9 includes additional features that are not included in Claim 1. Specifically, Claim 1 includes the feature of communication between an access point and a client terminal. Claim 2, on the other hand, is communication by a communication apparatus, that according to Claim 9 is an access point, and another communication apparatus that is not necessarily a client terminal. Thus, the two claims are not duplicates. Reconsideration and withdrawal of the objection are respectfully requested.

Claims 1 to 15 were rejected under 35 U.S.C. § 112, second paragraph, for alleged antecedence concerns. The points noted in the Office Action, while not conceded as being correct, have been attended to by amendment. Reconsideration and withdrawal of the § 112 rejections are respectfully requested.

Claims 1 to 15 were rejected under 35 U.S.C. § 102(e) over U.S. Patent No. 6,920,559 (Nessett), and Claims 2, 6, 7, 11, 12, 14 and 15 were also been rejected under 35 U.S.C. § 102(b) over "Specification of the Bluetooth System" (Bluetooth). Reconsideration and withdrawal of the rejections are respectfully requested.

In the present invention, a first encrypted communication that does not require an authentication process is performed between an access point and a client terminal via an established wireless link, and then authentication data is sent by the access point to the client terminal while the first link is established. The first link is then discarded in response to the sending of the authentication data. Then, a second link that requires an authentication process is established using the authentication data sent to the client terminal, while the first link is continually discarded.

Referring specifically to the claims, Claim 1 is directed to a network configuration method comprising a first link establishing step of establishing, between an access point device and a client terminal, a wireless communication link through a first encrypted communication requiring no authentication process, a sending step of sending authentication data from the access point device to the client terminal in a state where the wireless communication link through the first encrypted communication is established, a link discarding step of discarding the wireless communication link through the first encrypted communication between the access point device and the client terminal in response to the sending of the authentication data at the sending step, and a second link establishing step of establishing, between the access point device and the client terminal, a wireless communication link through a second encrypted communication that requires an authentication process using the authentication data sent to the client terminal, continually discarding the link at the link discarding step.

Claim 2 is a method claim for a communication apparatus, while Claim 13 is a system claim and Claim 14 is an apparatus claim, each of which substantially corresponds to Claim 1.

Claim 11 is directed to a network configuration method for a communication apparatus, comprising a first link establishing step of establishing, between the communication apparatus and another communication apparatus, a wireless communication link through a first encrypted communication requiring no authentication process, a receiving step of receiving authentication data from the another communication apparatus in a state where the wireless communication link at the first link establishing step is established, a link discarding step of discarding the wireless communication link established at the first link establishing step between the communication apparatus and the another communication apparatus in response to the receiving of the authentication data at the receiving step, and a second link establishing step of establishing, between the communication apparatus and the another communication apparatus, a wireless communication link through a second encrypted communication that requires an authentication process using the authentication data received from the another communication apparatus, continually discarding the link at the link discarding step.

Claim 15 is an apparatus claim that substantially corresponds to Claim 11.

The applied art is not seen to disclose or to suggest the features of Claims 1, 2, 11 and 13 to 15, and in particular, is not seen to disclose or to suggest at least the features of a first link establishing step of establishing, between a communication apparatus and another communication apparatus, a wireless communication link through a first encrypted communication requiring no authentication process, discarding the wireless communication link established at the first link establishing step in response to sending/ receiving of authentication data, and a second link establishing step of establishing, between the communication apparatus and the another communication apparatus, a

wireless communication link through a second encrypted communication that requires an authentication process using the authentication data received from the another communication apparatus, continually discarding the link at the link discarding step.

Nessett merely discloses that a wireless client completes a primary (complex) authentication protocol with and access point. Then, when the client is required to authenticate with another access point, it uses a secondary (less complex) authentication protocol. However, the client is required to periodically complete the primary authentication protocol so as to guard against unauthorized uses. However, Nessett is not seen to disclose or to suggest at least the features of a first link establishing step of establishing, between a communication apparatus and another communication apparatus, a wireless communication link through a first encrypted communication requiring no authentication process, discarding the wireless communication link established at the first link establishing step in response to sending/ receiving of authentication data, and a second link establishing step of establishing, between the communication apparatus and the another communication apparatus, a wireless communication link through a second encrypted communication that requires an authentication process using the authentication data received from the another communication apparatus, continually discarding the link at the link discarding step. Accordingly, Claims 1 to 15 are not believed to be anticipated by Nessett.

Bluetooth merely teaches the use of encryption keys and an authentication key in wireless communications. However, the Bluetooth standard is not seen to teach at least the features of a first link establishing step of establishing, between a communication apparatus and another communication apparatus, a wireless communication link through a

first encrypted communication requiring no authentication process, discarding the wireless communication link established at the first link establishing step in response to sending/ receiving of authentication data, and a second link establishing step of establishing, between the communication apparatus and the another communication apparatus, a wireless communication link through a second encrypted communication that requires an authentication process using the authentication data received from the another communication apparatus, continually discarding the link at the link discarding step.

In view of the forgoing amendments and remarks, all of Claims 1 to 15 are believed to be allowable.

No other matters having been raised, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

/Edward Kmett/

Edward A. Kmett
Attorney for Applicant
Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 127877v1